APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/813,248	03/30/2004	Plinio Pimentel	3408.2.8	4822

21552   7590   11/23/2009
AUSTIN RAPP & HARDMAN
170 South Main Street, Suite 735
SALT LAKE CITY, UT 84101

EXAMINER
OKEKE, IZUNNA

ART UNIT	PAPER NUMBER
2432	

NOTIFICATION DATE	DELIVERY MODE
11/23/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

usptocorrespondence@austin-rapp.com

	Application No.	Applicant(s)
Office Action Summary	10/813,248	PIMENTEL, PLINIO
	Examiner	Art Unit	
	IZUNNA OKEKE	2432	

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on <u>07 August 2009</u>.

2a) ☒ This action is FINAL.　　2b) ☐ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) <u>1-20</u> is/are pending in the application.

　　4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) <u>1-20</u> is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.

　　Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

　　Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

　　a) ☐ All　b) ☐ Some * c) ☐ None of:

　　　　1. ☐ Certified copies of the priority documents have been received.

　　　　2. ☐ Certified copies of the priority documents have been received in Application No. _____.

　　　　3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

　　* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08)　Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)　Paper No(s)/Mail Date. _____
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1.   Applicant's arguments filed 08/07/2009 have been fully considered but they are not

persuasive.

        Applicant's amended claim now recites the limitation "wherein the at least one sensitive

file continues to be stored on the computing system". The applicant argues that McBrearty

destroys the file if the access attempt to the file is not on an authorized connection list. Examiner

agrees that McBrearty destroys the file which meets applicant's limitation in claim 1 of

"performing an access prevention task". The file is destroyed because McBrearty maintains an

exact copy of the file and restores the file from the copy after destroying or deleting the original

file.

        The secondary reference (Vainstein US-6889210) was used to teach the other access

prevention tasks of encrypting the file or locking the file as recited in claim 6 with the rational

that McBrearty employing such access prevention technique (encrypting or locking the file) will

continue to store the file on the computing system (instead of maintaining a backup copy of the

file) by encrypting or locking the file should an unauthorized connection be made to the file. So,

the limitation in amended claim 1 is already addressed by the secondary reference because

encrypting or locking the file maintains the file on the system and does not destroy the file.

Claim Rejections - 35 USC § 103

2.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

        (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
        section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are
        such that the subject matter as a whole would have been obvious at the time the invention was made to a person

having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the
manner in which the invention was made.

3.   Claims 1-3 and 5-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over

McBrearty et al. (US-20020129152), and further in view of Vainstein (US-6889210).

a.   _Referring to claim 1, 13, 15 and 18:_

        Regarding claim 1, McBrearty teaches in a computing device, a method for protecting

sensitive files from unauthorized access, comprising:

detecting a connection of the computing device to an electronic device; accessing an authorized

connection list (See McBrearty, Para 21 teaches a connection a device to a web resource and

accessing an authorized list to determine if the user or connection is authorized);

determining whether the connection is identified in the authorized connection list (Para 21

teaches comparing the connection to an authorized list to determine if it is an authorized

connection); and

if the connection is not identified in the authorized connection list; accessing sensitive file

information which identifies at least one sensitive file stored on the computing device (See

McBrearty, Para 21-22 teaches if the user is not authorized to access a sensitive file stored on the

server); and

preventing access to the at least one sensitive file identified by the sensitive file information by

performing an access prevention task after the connection is not identified in the authorized

connection list (See McBrearty, Para 21-22 teaches a protection process of preventing access to

the sensitive file by performing an access protection task such as deleting the file or making it

inaccessible).

McBrearty teaches maintaining a copy of the sensitive file on the computing system but does not teach maintaining the original sensitive file on the computing system by encrypting or locking the file as an access prevention task.

However, Vainstein teaches a method of maintaining a sensitive file on a computing system and encrypting, locking or moving the file to a protected storage to prevent access to the file when an unauthorized user seeks access to the file (See Vainstein, Col 5, Line 63-67 teaches protecting a sensitive file by encryption or locking the file with a file key or writing it into a protected storage).

Therefore, it would have been obvious to modify McBrearty's access prevention task to also include an option of encrypting the file or locking the file or moving the file to a protected storage (instead of deleting the file) to protect and prevent access to the file while it is stored on the computing device thereby making the system more efficient by eliminating the need to maintain backups of the sensitive file.

a.   *Referring to claim 2, 16 and 19:*

Regarding claim 2, the combination of McBrearty and Vainstein teaches the method of claim 1, wherein if the connection is not identified in the authorized connection list the method further comprises: detecting termination of the connection; and if the computing device does not have any other unauthorized connections, restoring access to the at least one sensitive file identified by the sensitive file information (See McBrearty, Para 25 teaches restoring the file after the protection process).

a.   *Referring to claim 3:*

Regarding claim 3, the combination of McBrearty and Vainstein teaches the method of

claim 1, wherein the connection occurs via a computer network (See McBrearty, Para 16-18

teaches a computer network connection).

a.   *Referring to claim 5:*

Regarding claim 5, the combination of McBrearty and Vainstein teaches the method of

claim 1, wherein the connection is a direct connection (See McBrearty, Para 16 and18 teaches a

direct a connection of a host to a server).

a.   *Referring to claim 6-8, 17 and 20:*

Regarding claim 5, the combination of McBrearty and Vainstein teaches the method of

claim 1, wherein the access prevention task comprises locking the at least one sensitive file,

encrypting the at least one sensitive file or moving the at least one sensitive file to a host-

protected area of the storage device (See Vainstein, Col 5, Line 63-67 teaches protecting a

sensitive file by encryption or locking the file with a file key or writing it into a protected

storage)

a.   *Referring to claim 9:*

Regarding claim 9, the combination of McBrearty and Vainstein teaches the method of

claim 1, wherein the sensitive file information is a reference to a directory in which the at least

one sensitive file is stored (See Vainstein, Col 7, Line 17-31 teaches a header file structure linked

to the protective file which references or points to the location of the protected file).

a.   *Referring to claim 10:*

Regarding claim 10, the combination of McBrearty and Vainstein teaches the method of

claim 1, wherein the sensitive file information is a list of the at least one sensitive file (See

McBrearty, Para 21 teaches parameters relating to the protected file).

a.   *Referring to claim 11:*

Regarding claim 11, the combination of McBrearty and Vainstein teaches the method of

claim 1, wherein the authorized connection list comprises a list of at least one authorized network

(See McBrearty, Para 21 teaches a list of authorized users on a network).

a.   *Referring to claim 12:*

Regarding claim 12, the combination of McBrearty and Vainstein teaches the method of

claim 1, wherein the authorized connection list comprises a list of at least one authorized

connection type (See McBrearty, Para 21 teaches a list of authorized connections).

a.   *Referring to claim 14:*

Regarding claim 14, the combination of McBrearty and Vainstein teaches the method of

claim 13, further comprising: providing the authorized connection list; providing the sensitive

file information; and transmitting the authorized connection list and the sensitive file information

to the plurality of computing devices via the enterprise network (See McBrearty, Para 21-23

teaches providing the authorized connection list and parameters relating to protected files to the

server computers storing the sensitive files).

4.   Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over McBrearty et al.

(US-20020129152), and further in view of Elliott et al. (US-20030056095).

a.   *Referring to claim 4:*

Regarding claim 4, the combination of McBrearty and Vainstein teaches the method of

claim 3.

McBrearty does not teach the connection network as a wireless network and the device as

a mobile device.

However, Elliott teaches a method of securing encrypted files from unauthorized access

where the connection is made through a wireless network and by a mobile device (See Elliott,

Para 22)

Therefore, it would have been obvious to modify McBrearty's method and invention to

include support for a wireless network and a mobile device as the client as taught by Elliott for

the purpose of improving the system by incorporating wireless devices as client device making

request for access to files on the sever.

Conclusion

5.   Applicant's amendment necessitated the new ground(s) of rejection presented in this

Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a).

Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within TWO

MONTHS of the mailing date of this final action and the advisory action is not mailed until after

the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37

CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to IZUNNA OKEKE whose telephone number is (571)270-3854. The examiner can normally be reached on 9:00am - 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/I. O./
Examiner, Art Unit 2432

/Jung Kim/
Primary Examiner, AU 2432